Introduction to Computer Science
HW #3
Due: 2010/04/13

Chapter 4 Review Problems:

Problems 1, 7, 17, 20, 24, 37, 39, 40.

Programming Problem:

First, VERY IMPORTANT: check if sizeof(unsigned long long int) is 8. If not, use another computer.

Write two pieces of code:

(a) cipher.cpp reads the file "plain.txt" containing one string (length < 10000) and "public_key.txt" containing *N* and *e*. cipher.cpp should then output "secret.txt" as integers encrypted by RSA. The encoding concatenates 4 chars into one big integer and **multiply by 2**. For example, "ABCD" would be encoded as $2*(65*2^{24}+66*2^{16}+67*2^{8}+68)=2,189,723,272$. If the number of remaining chars is less than 4, put them as leftmost. For example, "A" would be encoded as $2*65*2^{24}=2,181,038,080$.

(b) decipher.cpp reads the file "secret.txt" and "private_key.txt" containing *N* and *d*. decipher.cpp should then output "message.txt" same as "plain.txt".

Note: Be careful about overflow, signed/unsigned, and eof() problem.

How to submit:

Compress all your files into one single file and then submit electronically via Ceiba by the due date.